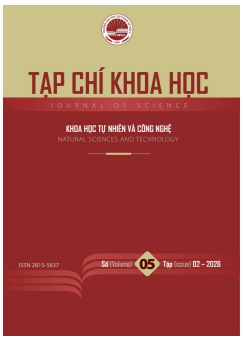
HPU2 Journal of Sciences:
Natural Sciences and Technology

Journal homepage: https://sj.hpu2.edu.vn



Article type: Research article

Structural cryptanalysis and storage efficiency of Kronecker-product diffusion layers for lightweight block ciphers

Thi-Tuyet Phan*

Electric Power University, Hanoi, Vietnam

Abstract

Matrix-based linear transformations are fundamental to the diffusion properties of modern block ciphers. This paper investigates the algebraic structure and security of the Dual-Matrix Affine Modular construction $C \equiv K_L M K_R + K_S \pmod{p}$. Although it is structurally isomorphic to a constrained affine map on $\mathbb{Z}_p^{n^2}$ via the Kronecker product $K_R^{\mathsf{T}} \otimes K_L$, this construction offers a significant efficiency advantage: it reduces the storage complexity from $\mathcal{O}(n^4)$ (for a generic linear layer) to $\mathcal{O}(n^2)$. We formally derive the effective key space and present a rigorous structural chosen-plaintext attack. We prove that by exploiting the tensor decomposition property, an equivalent key tuple can be recovered in $\mathcal{O}(n^4)$ field operations, significantly bypassing the $\mathcal{O}(n^6)$ complexity of generic affine cryptanalysis. Our results demonstrate that while insecure as a standalone primitive, this structure offers a favorable trade-off between large-state diffusion and implementation cost, making it a compelling candidate for the mixing layer in lightweight Substitution-Permutation Networks (SPNs).

Keywords: Linear algebra, matrix cryptography, dual-affine cipher, finite fields, modular arithmetic, Kronecker product, information security

1. Introduction

The interplay between linear algebra and cryptography has a long history. Early classical ciphers, such as the polygraphic substitution system introduced by Hill in 1929 [1], demonstrated that square matrices over finite rings could be used to diffuse plaintext data efficiently. Over the ensuing decades, this idea matured into modern block ciphers, culminating in the Advanced Encryption Standard (AES), which combines invertible linear transformations with nonlinear S-boxes [2], [3]. Comprehensive treatments of cryptography emphasise that robust schemes must balance diffusion provided by linear

* Corresponding author, E-mail: tuyetpt@epu.edu.vn

https://doi.org/10.56764/hpu2.jos.2026.5.2.65-83

Received date: 02-3-2026 ; Revised date: 07-6-2026 ; Accepted date: 07-8-2026

This is licensed under the CC BY-NC 4.0

layers with confusion supplied by nonlinear components, a principle tracing back to Shannon's foundational theory [4], [5]. These concepts are further detailed in standard texts [6], [7], [8], [9]. Fundamental results in matrix theory and finite fields underpin every aspect of block cipher design [10-11].

Despite the elegance of the Hill cipher, one-sided matrix multiplication over a finite field yields a small key space and exposes the scheme to established known-plaintext attacks. Differential and linear cryptanalysis, pioneered by Biham and Shamir [12] and Matsui [13], exploit linear relations in block ciphers to recover keys with complexity significantly lower than exhaustive search. Public-key cryptography, introduced by Diffie and Hellman [14], moved away from linear transformations toward number theoretic problems, but symmetric primitives remain an essential building block for secure communication.

Modern cryptographic standards formalise and refine these techniques. The U.S. National Institute of Standards and Technology (NIST) publishes Federal Information Processing Standards and Special Publications that define block cipher modes of operation [15, 16], randomness generation for dynamic keys [17], and digital signature algorithms [18]. These documents emphasise careful use of linear transformations and randomness to achieve confidentiality, integrity, and authenticity. Researchers have also proposed novel cipher structures that leverage two-sided matrix actions. For example, the ambiguous multi-symmetric scheme [19] encodes multiple plaintexts into one ciphertext using dual-matrix multiplication, and more recent work on tropical algebra uses matrix semirings for asymmetric cryptography [20]. However, as demonstrated in cryptanalytic studies of matrix-based schemes [21], algebraic structures often contain hidden linear structures that allows for equivalent key recovery, necessitating rigorous structural evaluation.

In this paper, we revisit matrix-based cryptography from the perspective of structural efficiency. We analyze the Dual-Matrix Affine Modular map not as a standalone cipher but rather as a candidate for high-efficiency diffusion. Unlike standard Maximum Distance Separable (MDS) matrices which impose high storage overheads (n^4 elements for a state of size n^2), the dual-matrix scheme employs a Kronecker-product structure to operate on n^2 -dimensional vectors using only $3n^2$ parameters (comprising K_L, K_R, K_S). The main contributions of this work are as follows:

1. We derive the exact number of distinct encryption functions $|\mathcal{K}_{\text{eff}}| = \frac{|\mathrm{GL}_n(\mathbb{Z}_p)|^2 . p^{n^2}}{p-1}$, and the corresponding asymptotic growth in p and n.

2. We distinguish between generic affine attacks $O(n^6)$ and structural attacks. We prove that by exploiting the Kronecker structure, the key can be recovered in $O(n^4)$ time using a chosen-plaintext attack based on simultaneous conjugation.

3. We demonstrate that this structure provides a cubic encryption complexity $O(n^3)$ for a state size of n^2, asymptotically more efficient than the $O(n^4)$ complexity of standard diffusion layers.

The remainder of this article is organised as follows. Section 2 reviews linear algebraic preliminaries, including finite fields, matrix spaces, and the Kronecker product. Section 3 surveys classical matrix-based ciphers and their cryptanalytic limitations. Section 4 formally defines the DMAMC scheme, proves correctness, and analyses the size of its key space. Section 5 evaluates the complexity of generic and structural attacks, highlighting the role of two-sided multiplication. Section 7 provides worked examples to demonstrate the scheme in practice. Finally, Section 8 summarises the work and discusses avenues for future research.

Notation: Throughout the paper, p denotes a prime and $\mathbb{Z}_p = \mathbb{Z}_p$ is the finite field of integers modulo p. Equivalently, we write $\mathbb{F}_p = \mathbb{Z}/\mathrm{p}\mathbb{Z}$ for this finite field. For $n \in \mathbb{N}$, $M_n(\mathbb{Z}_p) = M_n(\mathbb{Z}_p)$ denotes the ring of all $n \times n$ matrices over $\mathbb{Z}_p$, and $\mathrm{GL}_n(\mathbb{Z}_p) = \mathrm{GL}_n(\mathbb{Z}_p) = \{A \in M_n(\mathbb{Z}_p) | \det(A) \not\equiv 0 \pmod p\}$ denotes the general linear group. The identity and zero matrices of size n are denoted by I_n and $0_{n\times n}$, respectively. For matrices (or scalars) A, B over $\mathbb{Z}_p$, the congruence $A \equiv B \pmod p$ is interpreted entrywise. For $A \in \mathrm{GL}_n(\mathbb{Z}_p)$, the modular inverse is denoted by A^{-1}, i.e., $AA^{-1} \equiv A^{-1}A \equiv I_n \pmod p$; $adj(A)$ denotes the adjugate matrix of A. The transpose of A is $A^\top$. The operator $diag(a_1, \dots, a_n)$ denotes the $n \times n$ diagonal matrix with diagonal entries $a_1, \dots, a_n$. The vectorisation operator $vec: M_n(\mathbb{Z}_p) \to \mathbb{Z}_p^{n^2}$ stacks the columns of a matrix into a single column vector. The Kronecker product is denoted by $\otimes$; in particular, for $A, B, X \in M_n(\mathbb{Z}_p)$ we use the identity $vec(AXB) = (B^\top \otimes A)vec(X)$. The plaintext space and ciphertext space are both $\mathcal{P} = \mathcal{C} = M_n(\mathbb{Z}_p)$. A secret key is $\mathcal{K} = (K_L, K_R, K_S)$ with $K_L, K_R \in \mathrm{GL}_n(\mathbb{Z}_p)$ and $K_S \in M_n(\mathbb{Z}_p)$, and the DMAMC encryption map is $E_{\mathcal{K}}(M) \equiv K_L M K_R + K_S \pmod p$. We write $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash \{0\}$ for the multiplicative group of $\mathbb{Z}_p$. Finally, the dimension of the vectorised state is denoted by $N := n^2$, and asymptotic costs are expressed using $O(\cdot)$ in the number of field operations over $\mathbb{Z}_p$. The all-ones matrix of size n is denoted by J_n.

2. Linear Algebra Preliminaries over Finite Fields

To ensure deterministic encryption and decryption without precision loss, we operate strictly over finite fields rather than over $\mathbb{R}$.

Definition 2.1 Let p be a prime number. The finite field $\mathbb{Z}_p$ consists of the set of integers

$$\{0,1, \dots, p-1\},$$

equipped with addition and multiplication modulo p. Every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse.

Definition 2.2 Let $M_n(\mathbb{Z}_p)$ denote the ring of $n \times n$ matrices with entries in $\mathbb{Z}_p$. The general linear group of degree n over $\mathbb{Z}_p$ is defined by

$$\mathrm{GL}_n(\mathbb{Z}_p) = \{A \in M_n(\mathbb{Z}_p) | \det(A) \not\equiv 0 \pmod p\}.$$

Elements of $GL_n(\mathbb{Z}_p)$ are precisely the invertible matrices over $\mathbb{Z}_p$.

Definition 2.3 Let $A \in GL_n(\mathbb{Z}_p)$. The inverse matrix A^{-1} over $\mathbb{Z}_p$ is the unique matrix satisfying

$$AA^{-1} \equiv A^{-1}A \equiv I_n \pmod p,$$

where I_n denotes the $n \times n$ identity matrix. Fundamental properties of matrix inverses over finite fields are discussed in [10], [11], [22], [23]; see also [26] for an elementary cryptanalytic treatment. If $det(A) \not\equiv 0 \ (mod\ p)$, then

$$A^{-1} \equiv (\det(A))^{-1} \cdot adj(A) \pmod p, \tag{1}$$

where $(det(A))^{-1}$ denotes the multiplicative inverse of $det(A)$ in $\mathbb{Z}_p$ and $adj(A)$ denotes the adjugate matrix of A. The scalar $(det(A))^{-1}$ can be computed using the Extended Euclidean Algorithm [22].

To analyse the global linear structure of the proposed cipher, we use the vectorisation operator and the Kronecker product.

Definition 2.4 For $X = [x_{ij}] \in M_n(\mathbb{Z}_p)$, the vectorisation operator $vec: M_n(\mathbb{Z}_p) \to \mathbb{Z}_p^{n^2}$ stacks the columns of X into a single column vector:

$$vec(X) = (x_{11}, x_{21}, \dots, x_{n1}, x_{12}, \dots, x_{n2}, \dots, x_{1n}, \dots, x_{nn})^\top.$$

This map is a linear isomorphism between $M_n(\mathbb{Z}_p)$ (as a vector space over $\mathbb{Z}_p$) and $\mathbb{Z}_p^{n^2}$.

Lemma 2.1 Let $A, B, X \in M_n(\mathbb{Z}_p)$. The vectorisation operator $vec: M_n(\mathbb{Z}_p) \to \mathbb{Z}_p^{n^2}$ satisfies the identity:

$$vec(AXB) = (B^\top \otimes A)\, vec(X). \tag{2}$$

In particular, if $A, B \in GL_n(\mathbb{Z}_p)$, then $B^\top \otimes A \in GL_{n^2}(\mathbb{Z}_p)$, since

$$\det(B^\top \otimes A) = (\det B)^n (\det A)^n \not\equiv 0 \pmod p.$$

Theorem 2.1 *For each pair $(K_L, K_R) \in GL_n(\mathbb{Z}_p) \times GL_n(\mathbb{Z}_p)$, the map*

$$T_{K_L,K_R}: M_n(\mathbb{Z}_p) \longrightarrow M_n(\mathbb{Z}_p), \qquad T_{K_L,K_R}(M) = K_L M K_R,$$

is a linear automorphism on $M_n(\mathbb{Z}_p)$. Moreover, if

$$\Phi: \mathrm{GL}_n(\mathbb{Z}_p) \times \mathrm{GL}_n(\mathbb{Z}_p) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(M_n(\mathbb{Z}_p)), \qquad \Phi(K_L, K_R) := T_{K_L,K_R}.$$

Define the (action) kernel by

$$\ker(\Phi) := \{(K_L, K_R) \in \mathrm{GL}_n(\mathbb{Z}_p) \times \mathrm{GL}_n(\mathbb{Z}_p) \mid T_{K_L,K_R} = \mathrm{id}_{M_n(\mathbb{Z}_p)}\}.$$

Then

$$\ker(\Phi) = \{(\lambda I_n, \lambda^{-1} I_n) \mid \lambda \in \mathbb{Z}_p^\times\}.$$

Proof. Linearity of T_{K_L,K_R} follows immediately from the distributivity of matrix multiplication over addition and compatibility with scalar multiplication. Since $K_L, K_R \in \mathrm{GL}_n(\mathbb{Z}_p)$, the map T_{K_L,K_R} admits an explicit inverse given by

$$T_{K_L,K_R}^{-1}(M) = K_L^{-1} M K_R^{-1}, \qquad M \in M_n(\mathbb{Z}_p),$$

so T_{K_L,K_R} is a bijective linear map, i.e., a linear automorphism on $M_n(\mathbb{Z}_p)$.

To determine the kernel of Φ, suppose $(K_L, K_R) \in \ker(\Phi)$. By definition, this means

$$T_{K_L,K_R}(M) = M \quad \text{for all } M \in M_n(\mathbb{Z}_p),$$

i.e.,

$$K_L M K_R = M \quad \text{for all } M \in M_n(\mathbb{Z}_p). \tag{3}$$

First, set $M = I_n$ in (3). We obtain

$$K_L K_R = I_n \quad \Longrightarrow \quad K_R = K_L^{-1}.$$

Substituting this into (3) yields

$$K_L M K_L^{-1} = M \quad \text{for all } M \in M_n(\mathbb{Z}_p),$$

or equivalently,

$$K_L M = M K_L \quad \text{for all } M \in M_n(\mathbb{Z}_p). \tag{4}$$

Thus K_L commutes with every matrix in $M_n(\mathbb{Z}_p)$.

Let E_{ij} denote the matrix whose (i,j)-entry is 1 and whose other entries are 0. Taking $M = E_{ij}$ in (4) for all i, j and comparing the entries of $K_L E_{ij}$ and $E_{ij} K_L$ shows that all off-diagonal entries of K_L must be zero and all diagonal entries must be equal. More explicitly, writing $K_L = (a_{kl})_{k,l=1}^n$:

• The condition $K_L E_{ij} = E_{ij} K_L$ for $i \neq j$ forces $a_{ij} = 0$ for all $i \neq j$.

• The same condition with $M = E_{ii}$ and $M = E_{jj}$ implies $a_{ii} = a_{jj}$ for all i, j.

Therefore K_L is a scalar matrix,

$$K_L = \lambda I_n \quad \text{for some } \lambda \in \mathbb{Z}_p.$$

Since $K_L \in \mathrm{GL}_n(\mathbb{Z}_p)$, its determinant is nonzero modulo p, so $\lambda \neq 0$, and hence $\lambda \in \mathbb{Z}_p^{\times} = \mathbb{Z}_p \backslash \{0\}$. Using $K_R = K_L^{-1}$, we obtain

$$K_R = (\lambda I_n)^{-1} = \lambda^{-1} I_n.$$

Thus every element of $\ker(\Phi)$ has the form $(\lambda I_n, \lambda^{-1} I_n)$ with $\lambda \in \mathbb{Z}_p^{\times}$.

Conversely, for any $\lambda \in \mathbb{Z}_p^{\times}$ and any $M \in M_n(\mathbb{Z}_p)$ we have

$$(\lambda I_n) M (\lambda^{-1} I_n) = \lambda \lambda^{-1} M = M,$$

so $(\lambda I_n, \lambda^{-1} I_n) \in \ker(\Phi)$. Hence

$$\ker(\Phi) = \{(\lambda I_n, \lambda^{-1} I_n) | \lambda \in \mathbb{Z}_p^{\times}\},$$

as claimed.

Remark 2.1 *In terms of vectorisation, T_{K_L, K_R} corresponds to the linear map*

$$vec(T_{K_L, K_R}(X)) = (K_R^{\top} \otimes K_L)\, vec(X),$$

where $K_R^{\top} \otimes K_L \in GL_{n^2}(\mathbb{Z}_p)$ is an invertible matrix over $\mathbb{Z}_p$ by Lemma 2.1.

3. Review of Matrix-Based Encryption Techniques

This section provides a brief overview of classical matrix-based techniques and motivates the proposed dual-transformation scheme.

Classical matrix-based ciphers

The Hill cipher. The Hill cipher partitions plaintext into vectors $v \in \mathbb{Z}_p^n$ and encrypts via

$$c \equiv Kv \pmod{p},$$

where $K \in \mathrm{GL}_n(\mathbb{Z}_p)$ and c is the ciphertext vector [1]. Classical cryptanalysis of such systems is detailed in [26]. Decryption is given by

$$v \equiv K^{-1} c \pmod{p}.$$

Although conceptually elegant and easy to implement, the Hill cipher is susceptible to known-plaintext attacks. If an adversary obtains n linearly independent plaintext–ciphertext pairs (v_i, c_i), they can form

$$V = [v_1 \ \cdots \ v_n], \quad C = [c_1 \ \cdots \ c_n],$$

and solve

$$C = KV \quad \Rightarrow \quad K = CV^{-1},$$

provided V is invertible over $\mathbb{Z}_p$.

Affine matrix ciphers. To avoid mapping the zero plaintext to zero ciphertext, affine variants introduce an additive shift:

$$c \equiv Av + b \pmod{p},$$

where $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ and $b \in \mathbb{Z}_p^n$. This eliminates the trivial relation $0 \mapsto 0$ and mitigates several obvious forms of structural leakage. However, the scheme remains vulnerable to differential analysis. For two plaintext vectors v_1, v_2 with ciphertexts c_1, c_2, we have

$$c_1 - c_2 \equiv A(v_1 - v_2) \pmod{p},$$

so the additive offset b is eliminated and the problem reduces to the linear Hill case. With sufficiently many independent differences, A can still be recovered efficiently [6].

Eigenvector-based and similarity transformations. A more sophisticated class of schemes employs similarity transformations of the form

$$C = P^{-1}MP + B,$$

where P is constructed from eigenvectors of some public matrix and B is an affine offset. The underlying idea is to use diagonalisation or Jordan forms to hide structure inside a transformed basis. However, these methods suffer from several limitations:

• They enforce the structural constraint $K_L = K_R^{-1}$ (since the transformation is a similarity), which reduces the size of the key space compared to fully independent left and right keys.

• Implementations over $\mathbb{R}$ or $\mathbb{C}$ are prone to numerical instability and rounding errors during decryption when P^{-1} is approximated in floating-point arithmetic.

• When reduced modulo p, the diagonalisation assumptions may fail (e.g., non-diagonalisable matrices over $\mathbb{Z}_p$), further constraining the design.

The DMAMC scheme proposed in this paper addresses these issues by:

(i) decoupling the left and right key matrices (equivalence transformation rather than similarity);

(ii) operating entirely over finite fields to guarantee exact arithmetic;

(iii) enlarging the key space by allowing independent K_L, K_R and an arbitrary affine shift K_S.

4. Dual-Matrix Affine Modular Cipher (DMAMC)

Definition of the DMAMC scheme

Let p be a prime modulus. (In Theorem 5.3 we additionally assume $p \geq n$ to choose n pairwise distinct elements in $\mathbb{Z}_p$). Messages are processed in blocks of size $n \times n$ over $\mathbb{Z}_p$.

• **Plaintext space**:

$$\mathcal{P} = M_n(\mathbb{Z}_p).$$

• **Ciphertext space**:

$$\mathcal{C} = M_n(\mathbb{Z}_p).$$

• **Key space**: a key is a triple

$$\mathcal{K} = (K_L, K_R, K_S),$$

where

$$K_L, K_R \in \mathrm{GL}_n(\mathbb{Z}_p), \qquad K_S \in M_n(\mathbb{Z}_p).$$

Definition 4.1 (Encryption**)** *Given a plaintext block $M \in \mathcal{P}$ and key $\mathcal{K} = (K_L, K_R, K_S)$, the encryption map $E_{\mathcal{K}}: \mathcal{P} \to \mathcal{C}$ is defined by*

$$C \equiv K_L M K_R + K_S \pmod{p}. \tag{5}$$

Definition 4.2 (Decryption**)** *Given a ciphertext block $C \in \mathcal{C}$ and key $\mathcal{K} = (K_L, K_R, K_S)$, the decryption map $D_{\mathcal{K}}: \mathcal{C} \to \mathcal{P}$ is defined by*

$$M \equiv K_L^{-1}(C - K_S)K_R^{-1} \pmod{p}. \tag{6}$$

Theorem 4.1 *For any $M \in \mathcal{P}$ and any key $\mathcal{K} = (K_L, K_R, K_S)$ with $K_L, K_R \in GL_n(\mathbb{Z}_p)$, the scheme satisfies*

$$D_{\mathcal{K}}(E_{\mathcal{K}}(M)) = M. \tag{7}$$

Proof. By definition, for any $M \in \mathcal{P}$ the encryption procedure outputs

$$E_{\mathcal{K}}(M) \equiv K_L M K_R + K_S \pmod{p}.$$

Applying the decryption map to this ciphertext yields

$$\begin{aligned} D_{\mathcal{K}}(E_{\mathcal{K}}(M)) &\equiv K_L^{-1}((K_L M K_R + K_S) - K_S)K_R^{-1} \pmod{p} \\ &= K_L^{-1}(K_L M K_R)K_R^{-1} \\ &= (K_L^{-1}K_L)M(K_R K_R^{-1}) \\ &= I_n M I_n = M. \end{aligned}$$

Since K_L and K_R are invertible over $\mathbb{Z}_p$, the inverses K_L^{-1} and K_R^{-1} exist and are unique, guaranteeing deterministic recovery of M.

Following the formal framework commonly used in matrix cryptography [21], we detail the operational procedures for key generation, encryption, and decryption in Algorithms 1, 2, and 3.

Remark 4.1 *The mapping $M \mapsto K_L M K_R$ is a group automorphism of the additive group $(M_n(\mathbb{Z}_p), +)$. Adding K_S produces an affine transformation on $M_n(\mathbb{Z}_p)$. Under vectorisation, the global map can be written as*

$$vec(C) = (K_R^{\top} \otimes K_L)vec(M) + vec(K_S).$$

This explicitly demonstrates that DMAMC is structurally isomorphic to a standard Affine Cipher over the larger vector space $\mathbb{Z}_p^{n^2}$, restricted to a subgroup of keys defined by Kronecker products.

Algorithm 1 DMAMC Key Generation

Input: Security parameter n (block size), large prime p.

Output: Secret key tuple $\mathcal{K} = (K_L, K_R, K_S)$.

1: **procedure** KEYGEN (n, p)

2: **repeat**

3: Select $K_L \in M_n(\mathbb{Z}_p)$ uniformly at random

4: **until** $\det(K_L) \not\equiv 0 \pmod{p}$

5: **repeat**

6: Select $K_R \in M_n(\mathbb{Z}_p)$ uniformly at random

7: **until** $\det(K_R) \not\equiv 0 \pmod{p}$

8: Select $K_S \in M_n(\mathbb{Z}_p)$ uniformly at random

9: **return** $\mathcal{K} \leftarrow (K_L, K_R, K_S)$

10: **end procedure**

Algorithm 2 DMAMC Encryption

Input: Plaintext matrix $M \in M_n(\mathbb{Z}_p)$, modulus p, key $\mathcal{K} = (K_L, K_R, K_S)$.

Output: Ciphertext matrix $C \in M_n(\mathbb{Z}_p)$.

1: **procedure** ENCRYPTION$(M, \mathcal{K})$

2: $T \leftarrow K_L M \pmod p$ Left diffusion

3: $T' \leftarrow TK_R \pmod p$ Right diffusion

4: $C \leftarrow T' + K_S \pmod p$ Affine shift

5: **return** C

6: **end procedure**

Algorithm 3 DMAMC Decryption

Input: Ciphertext matrix $C \in M_n(\mathbb{Z}_p)$, modulus p, key $\mathcal{K} = (K_L, K_R, K_S)$.

Output: Plaintext matrix $M \in M_n(\mathbb{Z}_p)$.

1: **procedure** DECRYPTION$(C, \mathcal{K})$

2: Compute $K_L^{-1} \pmod p$ and $K_R^{-1} \pmod p$

3: $T' \leftarrow C - K_S \pmod p$ Remove affine shift

4: $M \leftarrow K_L^{-1} T' K_R^{-1} \pmod p$ Invert linear map

5: **return** M

6: **end procedure**

5. Security and Complexity Analysis

5.1. Effective Key Space Size

A rigorous security evaluation must account for the redundancy identified in Theorem 2.1.

Theorem 5.1 Let $\mathcal{K}_{eff}$ denote the set of distinct affine encryption functions induced by the scheme. The cardinality of $\mathcal{K}_{eff}$ is exactly

$$|\mathcal{K}_{\text{eff}}| = \frac{|\mathrm{GL}_n(\mathbb{Z}_p)|^2 \cdot p^{n^2}}{p-1} = \frac{\left(\prod_{k=0}^{n-1}(p^n - p^k)\right)^2 p^{n^2}}{p-1}. \quad (8)$$

In particular, since

$$|\mathrm{GL}_n(\mathbb{Z}_p)| = p^{n^2} \prod_{k=1}^{n} (1 - p^{-k}),$$

the effective key space grows on the order of p^{3n^2-1} in the parameters p and n.

Proof. Consider the map

$$F: \mathrm{GL}_n(\mathbb{Z}_p) \times \mathrm{GL}_n(\mathbb{Z}_p) \times M_n(\mathbb{Z}_p) \longrightarrow \{\text{affine maps } M_n(\mathbb{Z}_p) \to M_n(\mathbb{Z}_p)\},$$

$$F(K_L, K_R, K_S)(M) = K_L M K_R + K_S.$$

Fixing a triple (K_L, K_R, K_S) determines an affine encryption function.

First, if $F(K_L, K_R, K_S) = F(K'_L, K'_R, K'_S)$, then evaluating both sides at $M = 0$ yields

$$K_S = F(K_L, K_R, K_S)(0) = F(K'_L, K'_R, K'_S)(0) = K'_S,$$

so the additive key K_S is uniquely determined by the affine map.

Thus two keys (K_L, K_R, K_S) and (K'_L, K'_R, K_S) induce the same encryption function if and only if their linear parts

$$T_{K_L,K_R}(M) = K_L M K_R \quad \text{and} \quad T_{K'_L,K'_R}(M) = K'_L M K'_R$$

coincide. This is precisely the situation of Theorem 2.1: the map

$$\Phi: \mathrm{GL}_n(\mathbb{Z}_p) \times \mathrm{GL}_n(\mathbb{Z}_p) \to \mathrm{Aut}_{\mathbb{Z}_p}(M_n(\mathbb{Z}_p)), \qquad \Phi(K_L, K_R) = T_{K_L,K_R},$$

has kernel of size $|\ker(\Phi)| = p - 1$. By Theorem 2.1, two pairs (K_L, K_R) and (K'_L, K'_R) induce the same linear map on $M_n(\mathbb{Z}_p)$ if and only if there exists a unique $\lambda \in \mathbb{Z}_p^{\times}$ such that

$$(K'_L, K'_R) = (\lambda K_L, \lambda^{-1} K_R).$$

Hence each induced linear map corresponds to exactly $p - 1$ key pairs. For each such linear map and each $K_S \in M_n(\mathbb{Z}_p)$, the affine map $M \mapsto K_L M K_R + K_S$ is distinct. Consequently, the total number of distinct encryption functions is

$$|\mathcal{K}_{\text{eff}}| = \frac{|\mathrm{GL}_n(\mathbb{Z}_p)|^2 \cdot p^{n^2}}{p - 1},$$

as claimed.

5.2. Algebraic Cryptanalysis Complexity

The system can be modelled as a global affine map over the vectorised message space. Writing

$$y = \mathcal{A}x + b, \tag{9}$$

where $x = vec(M) \in \mathbb{Z}_p^{n^2}$, $y = vec(C) \in \mathbb{Z}_p^{n^2}$, $\mathcal{A} = K_R^{\top} \otimes K_L \in \mathrm{GL}_{n^2}(\mathbb{Z}_p)$ and $b = vec(K_S) \in \mathbb{Z}_p^{n^2}$, we obtain a standard affine map on $\mathbb{Z}_p^{n^2}$.

Theorem 5.2 Let $N = n^2$ denote the dimension of the vectorised message space. To uniquely recover the global transformation matrix $\mathcal{A}$ and the offset b by treating DMAMC as an unknown affine map $y = \mathcal{A}x + b$ over $\mathbb{Z}_p^N$, an adversary needs:

- at least $N + 1 = n^2 + 1$ plaintext–ciphertext pairs (a data complexity lower bound);
- and can then reconstruct $\mathcal{A}$ using Gaussian elimination in

$$\mathcal{T}_{\text{attack}} = \mathcal{O}(N^3) = \mathcal{O}((n^2)^3) = \mathcal{O}(n^6)$$

field operations.

Proof. Let $x_i = vec(M_i) \in \mathbb{Z}_p^N$ and $y_i = vec(C_i) \in \mathbb{Z}_p^N$ for $i = 1, \ldots, K$, so that

$$y_i = \mathcal{A}x_i + b \quad \text{for } i = 1, \ldots, K.$$

Each pair (x_i, y_i) contributes N scalar linear equations in the N^2 unknown entries of $\mathcal{A}$ and the N unknown entries of b, for a total of $N^2 + N$ unknowns. Thus, in the generic case, at least K such that

$$KN \geq N^2 + N \quad \Longrightarrow \quad K \geq N + 1 = n^2 + 1$$

plaintext–ciphertext pairs are required to determine $(\mathcal{A}, b)$ uniquely. This yields the stated data complexity lower bound.

To estimate the computational cost, fix an index 0 and form the differences

$$\Delta x_i = x_i - x_0, \qquad \Delta y_i = y_i - y_0, \quad i = 1, \dots, N.$$

Then

$$\Delta y_i = y_i - y_0 = (\mathcal{A}x_i + b) - (\mathcal{A}x_0 + b) = \mathcal{A}(x_i - x_0) = \mathcal{A}\Delta x_i$$

for each i. If the N vectors $\Delta x_1, \dots, \Delta x_N$ are linearly independent (which an active adversary can enforce by choosing x_i), we can form the matrices

$$X = [\Delta x_1 \ \cdots \ \Delta x_N], \qquad Y = [\Delta y_1 \ \cdots \ \Delta y_N],$$

with $X \in \mathrm{GL}_N(\mathbb{Z}_p)$ and

$$Y = \mathcal{A}X.$$

It follows that

$$\mathcal{A} = YX^{-1}.$$

Computing X^{-1} via Gaussian elimination on an $N \times N$ matrix costs $O(N^3)$ field operations, and computing the product YX^{-1} costs another $O(N^3)$ operations. With $N = n^2$ this yields an overall complexity

$$O(N^3) = O((n^2)^3) = O(n^6).$$

Remark 5.1 The bound above is a generic worst-case estimate obtained by treating $\mathcal{A}$ as an arbitrary element of $GL_{n^2}(\mathbb{Z}_p)$ and ignoring its special Kronecker-product structure. It correctly upper bounds the cost of reconstructing the global affine map, but does not reflect the best possible structural attacks, which we analyse next.

Theorem 5.3 Let $\mathcal{K} = (K_L, K_R, K_S)$ be the secret key and assume the field size satisfies $p \geq n$. Given chosen-plaintext access, an adversary can recover an algebraically equivalent key in $\mathcal{O}(n^4)$ field operations using 4 structured queries. The arithmetic cost is dominated by solving n homogeneous linear systems of size $n \times n$ (to obtain eigenvectors), which is $\mathcal{O}(n^4)$ field operations using Gaussian elimination.

Proof. The recovery proceeds through the following constructive steps.

Step 1 (Affine Removal): Query $M_0 = 0$ and receive $C_0 = E_{\mathcal{K}}(M_0) \equiv K_S \pmod p$.

Step 2 (Linear Isolation): Query $M_1 = I_n$ and receive $C_1 = E_{\mathcal{K}}(M_1)$. Compute $P \equiv C_1 - C_0 \equiv K_L K_R \pmod p$. Define the derived oracle (all operations in $M_n(\mathbb{Z}_p)$ taken modulo p)

$$F(M) := (E_{\mathcal{K}}(M) - K_S)\, P^{-1} \pmod p,$$

where P^{-1} is the inverse of P in $\mathrm{GL}_n(\mathbb{Z}_p)$ (right-multiplication). Then $F(M) \equiv K_L M K_L^{-1} \pmod p$.

Step 3 (Eigenvector Extraction): Since $p \geq n$, choose distinct $\lambda_1, \dots, \lambda_n \in \mathbb{Z}_p$ and query $M_2 = diag(\lambda_1, \dots, \lambda_n)$. Let $A := F(M_2) = K_L M_2 K_L^{-1}$. For each i, compute a nonzero eigenvector $v_i \in \ker(A - \lambda_i I_n)$ by Gaussian elimination over $\mathbb{Z}_p$. Solving n linear systems of size $n \times n$ costs $n \cdot O(n^3) = O(n^4)$. Let $V = [v_1 \ \cdots \ v_n]$. Then $K_L = VD^{-1}$ for some unknown diagonal matrix D.

Step 4 (Ambiguity Resolution): Query $M_3 = J_n$ (all-ones matrix). Compute $\tilde{B} = V^{-1}F(M_3)V$. The identity $\tilde{B} = D^{-1}J_n D$ implies $(\tilde{B})_{ij} = d_j/d_i$. Fixing $d_1 = 1$, we recover D (hence K_L) up to the inherent scalar ambiguity. Finally set $K_R = K_L^{-1}P$.

We summarize the structural key-recovery procedure derived in Theorem 5.3, following the cryptanalytic methodology of [21], in Algorithm 4.

Algorithm 4 Structural Key-Recovery Attack on DMAMC (Chosen Plaintext)

Input: Oracle $E_{\mathcal{K}}$, dimension n, prime modulus p, with all arithmetic over $\mathbb{F}_p = \mathbb{Z}/\mathrm{p}\mathbb{Z}$ and $p \geq n$.

Output: An equivalent key tuple $\mathcal{K}_{\mathrm{eq}} = (\widetilde{K}_L, \widetilde{K}_R, K_S)$.

1: **procedure** ATTACKINGDMAMC ($E_{\mathcal{K}}$)

2: **Step 1: Recover affine shift**

3: Query $M_0 \leftarrow 0_{n\times n}$ and receive $C_0 \leftarrow E_{\mathcal{K}}(M_0)$

4: $K_S \leftarrow C_0$

5: **Step 2: Isolate linear component**

6: Query $M_1 \leftarrow I_n$ and receive $C_1 \leftarrow E_{\mathcal{K}}(M_1)$

7: $P \leftarrow C_1 - K_S \pmod p$ $P \equiv K_L K_R$

8: Define local oracle $F(M) \leftarrow (E_{\mathcal{K}}(M) - K_S)P^{-1}$

9: **Step 3: Extract eigenvectors (recover K_L up to scalars)**

10: Choose pairwise distinct $\lambda_1, \dots, \lambda_n \in \mathbb{F}_p$, which is feasible since $p \geq n$.

11: $M_2 \leftarrow diag(\lambda_1, \dots, \lambda_n)$

12: $A \leftarrow F(M_2)$ $A = K_L M_2 K_L^{-1}$

13: **for** $i \leftarrow 1$ **to** n **do**

14: Compute a nonzero $v_i \in \ker(A - \lambda_i I_n)$ over $\mathbb{F}_p$ (Gaussian elimination)

15: **end for**

16: $V \leftarrow [v_1 \ \cdots \ v_n]$

17: **Step 4: Resolve scalar ambiguity**

18: $M_3 \leftarrow J_n$ (all-ones matrix)

19: $B \leftarrow F(M_3)$

20: $\tilde{B} \leftarrow V^{-1}BV$

21: Set $d_1 \leftarrow 1$

22: **for** $j \leftarrow 2$ **to** n **do**

23: $d_j \leftarrow (\tilde{B})_{1j}$

24: **end for**

25: $D \leftarrow diag(d_1, \dots, d_n)$

26: **Step 5: Reconstruct equivalent keys**

27: $\widetilde{K}_L \leftarrow VD^{-1} (\mathrm{mod}\ p)$

28: $\widetilde{K}_R \leftarrow \widetilde{K}_L^{-1}P \pmod p$

29: **return** $(\widetilde{K}_L, \widetilde{K}_R, K_S)$

30**: end procedure**

Remark 5.2 This structural attack shows that, in a chosen-plaintext model, the effective algebraic security of DMAMC is governed by an $O(n^4)$ structural recovery procedure, dominated by solving n homogeneous linear systems of size $n \times n$ via Gaussian elimination, rather than by the generic $O(n^6)$ bound obtained by ignoring the Kronecker-product structure. In particular, DMAMC does not provide an

asymptotic security advantage over the classical Hill cipher; its primary value lies in illustrating two-sided matrix transformations and serving as a flexible diffusion layer within more elaborate non-linear cryptographic constructions.

Remark 5.3. Weak-key classes. Algorithm 4 gives an $O(n^4)$ upper bound for recovering an equivalent key when K_L and K_R are treated as unstructured invertible matrices over the finite field. This bound should not be interpreted as a lower bound for every admissible key. Although singular or low-rank matrices are excluded by the requirement $K_L, K_R \in GL_n(\mathbb{F}_p)$, invertible matrices with low-complexity structure may still form weak-key classes. For example, if K_L or K_R is diagonal, monomial, permutation-diagonal, triangular with small bandwidth, block diagonal, circulant, Toeplitz, repeated-pattern, or unusually sparse with only $O(n)$ nonzero entries, then part of the recovery may reduce to determining scaling, permutation, block-local, or low-dimensional parameters. In such cases, the practical attack cost may be lower than the generic $O(n^4)$ bound obtained by solving n independent $n \times n$ linear systems using Gaussian elimination.

Therefore, if DMAMC is used as a cryptographic component, the key-generation procedure should reject diagonal, monomial, highly sparse, block-diagonal, low-bandwidth, repeated-pattern, circulant/Toeplitz, and other visibly structured matrix forms. This warning does not make DMAMC secure as a standalone cipher; rather, it prevents avoidable reductions below the generic structural attack bound when the construction is deployed as a diffusion layer inside a nonlinear SPN.

6. Efficiency and Applicability Analysis

Although Section 5 demonstrates that the DMAMC structure is cryptographically weak without S-boxes, its algebraic structure offers significant advantages for diffusion layer design in SPN ciphers.

Computational Complexity Comparison

Consider a cryptographic state of size $N = n^2$ elements over $\mathbb{F}_p$.

• **Generic Linear Layer:** A standard mixing layer (e.g., a large MDS matrix) multiplies the state vector by an $N \times N$ matrix. The complexity is $N^2 = (n^2)^2 = n^4$ multiplications.

• **Dual-Matrix Layer:** The transformation $M \mapsto K_L M K_R$ involves two $n \times n$ matrix multiplications. The complexity is $2n^3$ multiplications.

Proposition 6.1 *For a state of size $N = n^2$, the Dual-Matrix structure reduces the diffusion complexity by a factor of $n/2$ compared to a generic linear transformation. For $n = 8$ (64-symbol state), this is a $4\times$ speedup.*

For lightweight cryptographic implementations (e.g., IoT device), memory efficiency is a critical design consideration. A generic linear layer requires storing $N^2 = n^4$ elements. The dual-matrix *linear* structure requires storing only $2n^2$ elements (for K_L and K_R), or $3n^2$ elements if the affine shift K_S is included. This represents a storage reduction from $O(N^2)$ to $O(N)$.

Table 1. Consolidated comparison between the generic affine structure and the DMAMC structure.

Criterion	Generic affine structure on a vectorized state	DMAMC structure	Cryptographic implication
Algebraic form	$y = Ax + b$, where $A \in GL_N(\mathbb{F}_p)$, $b \in \mathbb{F}_p^N$, and $N = n^2$.	$C = K_L M K_R + K_S$, equivalently $\mathrm{vec}(C) = (K_R^T \otimes K_L)\,\mathrm{vec}(M) + \mathrm{vec}(K_S)$.	DMAMC is a restricted affine family whose linear part has Kronecker-product structure.

Criterion	Generic affine structure on a vectorized state	DMAMC structure	Cryptographic implication
Linear-key storage	$N^2 = n^4$ field elements.	$2n^2$ field elements for K_L and K_R.	The linear-layer storage decreases from $O(n^4)$ to $O(n^2)$.
Total affine storage	$N^2 + N = n^4 + n^2$ field elements.	$3n^2$ field elements for K_L, K_R, and K_S.	DMAMC is more storage-efficient for lightweight implementations.
Evaluation cost	Dense matrix-vector evaluation costs $O(N^2) = O(n^4)$ field operations.	Two $n \times n$ matrix multiplications cost $O(n^3)$ field operations.	The evaluation cost decreases asymptotically from $O(n^4)$ to $O(n^3)$.
Generic affine recovery	Treating the map as an arbitrary affine transformation requires $N + 1 = n^2 + 1$ chosen plaintext–ciphertext pairs and $O(N^3) = O(n^6)$ field operations.	The Kronecker-product structure enables a structural chosen-plaintext key-recovery attack in $O(n^4)$ field operations.	The structural restriction improves implementation efficiency but also enables a faster attack.
Standalone security	Insecure as a standalone block cipher under sufficient known/chosen plaintexts.	Also insecure as a standalone primitive; Algorithm 4 exploits the two-sided multiplication structure.	Neither construction should be used alone as a modern secure block cipher.
Suitable use	General linear diffusion, but with high memory cost for large states.	Storage-efficient diffusion candidate inside nonlinear SPN constructions.	DMAMC should be combined with nonlinear S-boxes and should avoid weak-key matrix classes.

Table 1 summarizes the principal trade-off between the two structures. The DMAMC construction is not claimed to be secure as a standalone cipher. Its principal advantage is implementation efficiency: for a vectorized state of dimension $N = n^2$, the storage requirement is reduced from $O(n^4)$ to $O(n^2)$, and the evaluation cost is reduced from $O(n^4)$ to $O(n^3)$. However, the Kronecker-product restriction also enables the structural $O(n^4)$ chosen-plaintext recovery described in Algorithm 4. Therefore, DMAMC is best regarded as a lightweight diffusion layer to be combined with nonlinear components.

7. Numerical Examples

We now present fully worked examples in which the modular arithmetic has been carefully verified. Throughout, we use the alphabet mapping

$$\mathrm{A} \mapsto 0,\ \mathrm{B} \mapsto 1,\ \ldots,\ \mathrm{Z} \mapsto 25,\ \mathrm{Space} \mapsto 26,\ ? \mapsto 27,\ ! \mapsto 28. \tag{10}$$

Example 1: Basic $\mathbf{2 \times 2}$ Block ($\boldsymbol{n = 2}$)

Consider a simple message and key setup over $\mathbb{Z}_{29}$.

Parameters.

- Modulus: $p = 29$.
- Block size: $n = 2$.

Plaintext. Message: **"MATH".**

$$\mathrm{M} \mapsto 12, \quad \mathrm{A} \mapsto 0, \quad \mathrm{T} \mapsto 19, \quad \mathrm{H} \mapsto 7.$$

We group into a 2×2 matrix by rows:

$$M = \begin{bmatrix} 12 & 0 \\ 19 & 7 \end{bmatrix}.$$

Setup: Message **"MATH"** maps to $M = \begin{bmatrix} 12 & 0 \\ 19 & 7 \end{bmatrix}$. Keys:

$$K_L = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}, \quad K_R = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}, \quad K_S = \begin{bmatrix} 10 & 5 \\ 2 & 14 \end{bmatrix}.$$

We verify invertibility:

$$\det(K_L) = 3 \cdot 2 - 5 \cdot 1 = 1 \not\equiv 0 \pmod{29},$$
$$\det(K_R) = 4 \cdot 2 - 1 \cdot 3 = 5 \not\equiv 0 \pmod{29}.$$

Thus $K_L, K_R \in \mathrm{GL}_2(\mathbb{Z}_{29})$.

Encryption Step-by-Step

Step 1: Left Multiplication. Let $T = K_L M$.

$$T = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 12 & 0 \\ 19 & 7 \end{bmatrix} = \begin{bmatrix} 36+95 & 0+35 \\ 12+38 & 0+14 \end{bmatrix}$$
$$= \begin{bmatrix} 131 & 35 \\ 50 & 14 \end{bmatrix} \equiv \begin{bmatrix} 15 & 6 \\ 21 & 14 \end{bmatrix} \pmod{29}.$$

Step 2: Right Multiplication. Let $T' = TK_R$.

$$T' = \begin{bmatrix} 15 & 6 \\ 21 & 14 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 60+18 & 15+12 \\ 84+42 & 21+28 \end{bmatrix}$$
$$= \begin{bmatrix} 78 & 27 \\ 126 & 49 \end{bmatrix} \equiv \begin{bmatrix} 20 & 27 \\ 10 & 20 \end{bmatrix} \pmod{29}.$$

Step 3: Affine Shift. Finally, $C = T' + K_S$.

$$C = \begin{bmatrix} 20 & 27 \\ 10 & 20 \end{bmatrix} + \begin{bmatrix} 10 & 5 \\ 2 & 14 \end{bmatrix} = \begin{bmatrix} 30 & 32 \\ 12 & 34 \end{bmatrix}$$
$$\equiv \begin{bmatrix} 1 & 3 \\ 12 & 5 \end{bmatrix} \pmod{29}.$$

Mapping indices $(1,3,12,5)$ yields the ciphertext **"BDMF"**.

Decryption. We compute the inverses of K_L and K_R using the adjugate formula.

For

$$K_L = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix},$$

we have $\det(K_L) = 1$ and

$$adj(K_L) = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \equiv \begin{bmatrix} 2 & 24 \\ 28 & 3 \end{bmatrix} \pmod{29}.$$

Hence

$$K_L^{-1} \equiv \begin{bmatrix} 2 & 24 \\ 28 & 3 \end{bmatrix}.$$

For

$$K_R = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix},$$

we have $\det(K_R) = 5$ and $\det(K_R)^{-1} \equiv 6 \pmod{29}$ since $5 \cdot 6 = 30 \equiv 1 \pmod{29}$. The adjugate is

$$adj(K_R) = \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix} \equiv \begin{bmatrix} 2 & 28 \\ 26 & 4 \end{bmatrix} \pmod{29}.$$

Therefore

$$K_R^{-1} \equiv 6 \cdot \begin{bmatrix} 2 & 28 \\ 26 & 4 \end{bmatrix} = \begin{bmatrix} 12 & 168 \\ 156 & 24 \end{bmatrix} \equiv \begin{bmatrix} 12 & 23 \\ 11 & 24 \end{bmatrix} \pmod{29}.$$

To decrypt, compute

$$C - K_S = \begin{bmatrix} 1 & 3 \\ 12 & 5 \end{bmatrix} - \begin{bmatrix} 10 & 5 \\ 2 & 14 \end{bmatrix} = \begin{bmatrix} -9 & -2 \\ 10 & -9 \end{bmatrix} \equiv \begin{bmatrix} 20 & 27 \\ 10 & 20 \end{bmatrix} \pmod{29},$$

which matches T'.

Then

$$K_L^{-1}(C - K_S) = \begin{bmatrix} 2 & 24 \\ 28 & 3 \end{bmatrix} \begin{bmatrix} 20 & 27 \\ 10 & 20 \end{bmatrix} = \begin{bmatrix} 280 & 534 \\ 590 & 816 \end{bmatrix} \equiv \begin{bmatrix} 19 & 12 \\ 10 & 4 \end{bmatrix} \pmod{29}.$$

Finally,

$$\begin{bmatrix} 19 & 12 \\ 10 & 4 \end{bmatrix} K_R^{-1} = \begin{bmatrix} 360 & 725 \\ 164 & 326 \end{bmatrix} \equiv \begin{bmatrix} 12 & 0 \\ 19 & 7 \end{bmatrix} = M \pmod{29}.$$

Thus the original plaintext matrix (and hence the message **"MATH"**) is recovered exactly.

***Example 2: Multi-Block* $\mathbf{3 \times 3}$ *Encryption* ($\boldsymbol{n = 3}$)**

We next consider a more complex example in which a longer message into two 3×3 blocks.

Parameters.

- Modulus: $p = 29$.
- Block size: $n = 3$.

Plaintext. Consider the message

$$\text{"}\boldsymbol{LINEARALGEBRA}!!!\text{"},$$

which has 18 characters. We split it into two blocks of length 9:

- Block 1: **"LINEAR AL"**,
- Block 2: **"GEBRA !!!"**.

Using the fixed mapping:

$$\begin{array}{llll} \mathrm{L} \mapsto 11, & \mathrm{I} \mapsto 8, & \mathrm{N} \mapsto 13, & \mathrm{E} \mapsto 4, \\ \mathrm{A} \mapsto 0, & \mathrm{R} \mapsto 17, & \text{Space} \mapsto 26, & \\ \mathrm{G} \mapsto 6, & \mathrm{B} \mapsto 1, & ! \mapsto 28, & \end{array}$$

we obtain:

$$\text{"}\boldsymbol{LINEARAL}\text{"} \mapsto (11,8,13,4,0,17,26,0,11),$$

$$\text{"}\boldsymbol{GEBRA}!!!\text{"} \mapsto (6,4,1,17,0,26,28,28,28).$$

We arrange each block row-wise into 3×3 matrices:

$$M_1 = \begin{bmatrix} 11 & 8 & 13 \\ 4 & 0 & 17 \\ 26 & 0 & 11 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 6 & 4 & 1 \\ 17 & 0 & 26 \\ 28 & 28 & 28 \end{bmatrix}.$$

Keys. Let

$$K_L = \begin{bmatrix} 2 & 1 & 0 \\ 3 & 4 & 1 \\ 1 & 1 & 2 \end{bmatrix}, \quad K_R = \begin{bmatrix} 1 & 5 & 2 \\ 2 & 1 & 3 \\ 0 & 4 & 1 \end{bmatrix}, \quad K_S = \begin{bmatrix} 5 & 10 & 15 \\ 2 & 4 & 6 \\ 1 & 3 & 5 \end{bmatrix}.$$

A direct determinant calculation shows

$$\det(K_L) = 9 \not\equiv 0 \pmod{29}, \quad \det(K_R) = -5 \equiv 24 \not\equiv 0 \pmod{29},$$

so $K_L, K_R \in \mathrm{GL}_3(\mathbb{Z}_{29})$.

Block 1: "LINEAR AL"

First compute

$$T_1 = K_L M_1 \pmod{29}.$$

A direct multiplication yields

$$K_L M_1 = \begin{bmatrix} 26 & 16 & 43 \\ 75 & 24 & 118 \\ 67 & 8 & 52 \end{bmatrix},$$

so, reducing modulo 29,

$$T_1 \equiv \begin{bmatrix} 26 & 16 & 14 \\ 17 & 24 & 2 \\ 9 & 8 & 23 \end{bmatrix} \pmod{29}.$$

Next compute

$$T'_1 = T_1 K_R \pmod{29}.$$

We obtain

$$T'_1 = \begin{bmatrix} 0 & 28 & 27 \\ 7 & 1 & 21 \\ 25 & 0 & 7 \end{bmatrix} \pmod{29}.$$

Adding the shift K_S:

$$C_1 = T'_1 + K_S = \begin{bmatrix} 0 & 28 & 27 \\ 7 & 1 & 21 \\ 25 & 0 & 7 \end{bmatrix} + \begin{bmatrix} 5 & 10 & 15 \\ 2 & 4 & 6 \\ 1 & 3 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 38 & 42 \\ 9 & 5 & 27 \\ 26 & 3 & 12 \end{bmatrix}.$$

Reducing modulo 29:

$$38 \equiv 9, \quad 42 \equiv 13,$$

so

$$C_1 \equiv \begin{bmatrix} 5 & 9 & 13 \\ 9 & 5 & 27 \\ 26 & 3 & 12 \end{bmatrix} \pmod{29}.$$

Mapping each entry to a character:

$$\begin{array}{llllll} 5 & \mapsto \mathrm{F}, & 9 & \mapsto \mathrm{J}, & 13 & \mapsto \mathrm{N}, \\ 27 & \mapsto ?, & 26 & \mapsto \text{Space}, & 3 & \mapsto \mathrm{D}, \quad 12 \quad \mapsto \mathrm{M}. \end{array}$$

Reading row-wise, Block 1 ciphertext is

"***FJNJF? DM***".

Block 2: "GEBRA !!!"

Similarly, compute

$$T_2 = K_L M_2 \pmod{29}.$$

We obtain

$$K_L M_2 = \begin{bmatrix} 29 & 8 & 28 \\ 114 & 40 & 135 \\ 79 & 60 & 83 \end{bmatrix},$$

so modulo 29,

$$T_2 \equiv \begin{bmatrix} 0 & 8 & 28 \\ 27 & 11 & 19 \\ 21 & 2 & 25 \end{bmatrix} \pmod{29}.$$

Next,

$$T'_2 = T_2 K_R \pmod{29},$$

which yields

$$T'_2 \equiv \begin{bmatrix} 16 & 4 & 23 \\ 20 & 19 & 19 \\ 25 & 4 & 15 \end{bmatrix} \pmod{29}.$$

Add the affine shift:

$$C_2 = T'_2 + K_S = \begin{bmatrix} 16 & 4 & 23 \\ 20 & 19 & 19 \\ 25 & 4 & 15 \end{bmatrix} + \begin{bmatrix} 5 & 10 & 15 \\ 2 & 4 & 6 \\ 1 & 3 & 5 \end{bmatrix} = \begin{bmatrix} 21 & 14 & 38 \\ 22 & 23 & 25 \\ 26 & 7 & 20 \end{bmatrix}.$$

Reducing modulo 29:

$$38 \equiv 9,$$

so

$$C_2 \equiv \begin{bmatrix} 21 & 14 & 9 \\ 22 & 23 & 25 \\ 26 & 7 & 20 \end{bmatrix} \pmod{29}.$$

Mapping back to characters:

$$\begin{array}{llll} 21 \mapsto \text{V}, & 14 \mapsto \text{O}, & 9 \mapsto \text{J}, \\ 22 \mapsto \text{W}, & 23 \mapsto \text{X}, & 25 \mapsto \text{Z}, \\ 26 \mapsto \text{Space}, 7 \mapsto \text{H}, & 20 \mapsto \text{U}. \end{array}$$

Hence Block 2 ciphertext is

"***VOJWXZ HU***".

Overall ciphertext. Concatenating the two blocks, the full ciphertext corresponding to **"LINEAR ALGEBRA !!!"** is

"***FJNJF? DMVOJWXZ HU***".

Example 3: Structure of a Linear Attack

From the global affine representation (9), an adversary observing multiple plaintext–ciphertext pairs (M_i, C_i) can form differences

$$\Delta M_{ij} = M_i - M_j, \quad \Delta C_{ij} = C_i - C_j.$$

Vectorisation yields

$$vec(\Delta C_{ij}) = \mathcal{A}\, vec(\Delta M_{ij}),$$

where $\mathcal{A} = K_R^{\top} \otimes K_L$. For $n = 2$, the vectorised differences lie in $\mathbb{Z}_p^4$ and $\mathcal{A}$ is a 4×4 matrix:

$$\underbrace{\begin{bmatrix} \Delta y_1 \\ \Delta y_2 \\ \Delta y_3 \\ \Delta y_4 \end{bmatrix}}_{\Delta \mathbf{y}} = \underbrace{\begin{bmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \\ \mathcal{A}_{21} & \mathcal{A}_{22} & \mathcal{A}_{23} & \mathcal{A}_{24} \\ \mathcal{A}_{31} & \mathcal{A}_{32} & \mathcal{A}_{33} & \mathcal{A}_{34} \\ \mathcal{A}_{41} & \mathcal{A}_{42} & \mathcal{A}_{43} & \mathcal{A}_{44} \end{bmatrix}}_{\mathcal{A}} \underbrace{\begin{bmatrix} \Delta m_1 \\ \Delta m_2 \\ \Delta m_3 \\ \Delta m_4 \end{bmatrix}}_{\Delta \mathbf{x}}.$$

By collecting four linearly independent difference pairs (i.e., five plaintext–ciphertext blocks), an attacker can, in principle, solve for $\mathcal{A}$. For higher dimensions n, the dimension n^2 of the underlying vector space causes the generic linear system to grow quadratically, so if an adversary attacks the global

affine map directly and ignores the special two-sided structure, the data requirement is higher than in the standard Hill cipher. However, as discussed in Section 5, structural attacks can exploit that very structure to recover equivalent keys more efficiently.

8. Conclusions

This study has presented the Dual-Matrix Affine Modular Cipher (DMAMC), a linear-algebra-based encryption scheme defined over finite fields that employs two-sided multiplication and an affine shift. By generalising the encryption function to

$$C \equiv K_L M K_R + K_S \pmod{p},$$

the construction avoids the structural coupling constraints of similarity-based transformations, including restricted key spaces and numerical instability. We proved the bijectivity and correctness of the scheme, characterised its action via the Kronecker product on the vectorised matrix space, and quantified the number of distinct encryption functions, which equals $|\mathcal{K}_{\text{eff}}| = \frac{|\mathrm{GL}_n(\mathbb{Z}_p)|^2 . p^{n^2}}{p-1}$ and grows on the order of p^{3n^2-1} as $p \to \infty$ (for fixed n). Using rigorously verified numerical examples, including both 2×2 and 3×3 block ciphers, we demonstrated the exactness of modular arithmetic and the practicality of the approach for lightweight cryptographic applications. The analysis of linear-algebraic attacks shows that, although the scheme remains an affine linear cipher and is therefore vulnerable in principle to algebraic key-recovery techniques, its security is ultimately limited by structural attacks: a generic affine attack that ignores the Kronecker-product structure and treats DMAMC as an arbitrary affine map on $\mathbb{Z}_p^{n^2}$ has complexity $O(n^6)$, whereas a similarity-based attack exploiting the two-sided multiplication and the derived conjugation oracle recovers an equivalent key in $O(n^4)$ field operations (dominated by solving n linear systems of size $n \times n$ via Gaussian elimination), and can be reduced to $\tilde{O}(n^3)$ using optimized finite-field linear algebra routines. This is asymptotically smaller than the generic $O(n^6)$ affine recovery that ignores the Kronecker-product structure. Accordingly, the increase in block dimension and key-space size is best viewed as a pedagogical and design feature for diffusion layers, rather than as a mechanism for achieving modern, cryptanalytically hardened block-cipher security.

Future work will investigate the integration of nonlinear substitution layers (e.g., S-boxes). In such a design, DMAMC would serve as a generalised diffusion layer providing high branch numbers, while the nonlinear layer provides the necessary confusion to resist differential cryptanalysis. Another promising direction is to explore extended constructions (for example, incorporating transposition terms) that further complicate the algebraic structure of the linear layer; a rigorous cryptanalytic analysis of such variants is reserved for future work.

References

[1] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929, doi: 10.2307/2298294.

[2] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," FIPS 197, May 2023, doi: 10.6028/NIST.FIPS.197-upd1.

[3] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Berlin, Germany: Springer, 2002, doi: 10.1007/978-3-662-04722-4.

[4] C. E. Shannon, "A mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, pp. 379–423 and 623–656, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[5] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[6] D. R. Stinson and M. B. Paterson, *Cryptography: Theory and Practice*, 4th ed. Boca Raton, FL, USA: CRC Press, 2018, doi: 10.1201/9781315282497.

[7] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed. Boca Raton, FL, USA: Chapman and Hall/CRC, 2020, doi: 10.1201/9781351133036.

[8] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., New York, NY, USA: Wiley, 1996.

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Boston, MA, USA: Pearson, 2017.

[10] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2013, doi: 10.1017/CBO9781139020411.

[11] R. Lidl and H. Niederreiter, "Finite Fields," *Cambridge*, U.K.: Cambridge Univ. Press, Oct.1996, doi: 10.1017/CBO9780511525926.

[12] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, Jan. 1991, doi: 10.1007/BF00630563.

[13] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT '93*, Lecture Notes in Computer Science, vol. 765, T. Helleseth, Ed. Berlin, Germany: Springer-Verlag, 1994, pp. 386–397, doi: 10.1007/3-540-48285-7_33.

[14] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[15] M. Dworkin, "Recommendation for block cipher modes of operation: Methods and techniques," NIST Special Publication 800-38A, Dec. 2001, doi: 10.6028/NIST.SP.800-38A.

[16] M. Dworkin, "Recommendation for block cipher modes of operation: The CMAC Mode for Authentication," NIST Special Publication 800-38B, Jan. 2005, doi: 10.6028/NIST.SP.800-38B-2005.

[17] E. Barker and J. Kelsey, "Recommendation for random number generation using deterministic random bit generators," NIST Special Publication 800-90A Rev. 1, Jun. 2015, doi: 10.6028/NIST.SP.800-90Ar1.

[18] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," FIPS 186-5, Feb. 2023, doi: 10.6028/NIST.FIPS.186-5.

[19] R. Bassous, A. Mansour, R. Assous, H. Fu, Y. Zhu, and G. Corser, "Ambiguous multi-symmetric scheme and applications," *Journal of Information Security*, vol. 8, no. 4, pp. 383–401, Oct. 2017, doi: 10.4236/jis.2017.84024.

[20] H. Huang, W. Kong, and T. Xu, "Asymmetric cryptography based on the tropical Jones matrix," *Symmetry*, vol. 16, no. 4, Art. no. 456, Apr. 2024, doi: 10.3390/sym16040456.

[21] H. Huang, L. Deng, C. Li, and C. Pan, "Cryptanalysis of an encryption scheme using matrices over finite fields," *Chinese Journal of Electronics*, vol. 27, no. 2, pp. 293–296, Mar. 2018, doi: 10.1049/cje.2017.07.007.

[22] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, FL, USA: CRC Press, Dec. 2018, doi: 10.1201/9781439821916.

[23] H. Anton and C. Rorres, *Elementary Linear Algebra: Applications Version*, 11th ed., New York, NY, USA: Wiley, 2013.

[24] D. J. Bernstein, J. Buchmann, and E. Dahmen (Eds.), *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, doi: 10.1007/978-3-540-88702-7.

[25] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1991, doi: 10.1017/CBO9780511840371.

[26] A. Sinkov, *Elementary Cryptanalysis: A Mathematical Approach*, Washington, DC, USA: Mathematical Association of America, 2009, doi: 10.5948/UPO9780883859377.